Treasury Inspector General for Tax Administration

SENSITIVE DATA REMAIN AT RISK FROM THE USE OF UNAUTHORIZED WIRELESS TECHNOLOGY

Issued on March 28, 2007

Highlights

Highlights of Report Number: 2007-20-060 to the Internal Revenue Service Chief Information Officer and Chief, Mission Assurance and Security Services.

IMPACT ON TAXPAYERS

The use of wireless technology is growing at a phenomenal rate because of its convenience, affordability, and mobility; however, the use of wireless technology also poses significant security risks. If unauthorized wireless devices are installed and connected to the Internal Revenue Service (IRS) network, sensitive financial data for over 226 million taxpayers could be at risk.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our statutory audit coverage and is included in our Fiscal Year 2006 Annual Audit Plan. In 2003, TIGTA reported an unauthorized wireless application in one location that was directly connected to the IRS-wide internal network containing sensitive taxpayer information. This follow-up review was conducted to determine whether IRS assets are at risk from the use of unapproved wireless network devices and to evaluate the security controls over the one IRS-approved wireless network, the Enterprise Logistics Information Technology network.

WHAT TIGTA FOUND

The IRS recognizes the need to control and secure the use of wireless technology. To correct the deficiencies TIGTA reported in 2003, the IRS disconnected the unauthorized wireless network and developed a comprehensive wireless security policy.

For this review, TIGTA scanned 20 IRS buildings in 10 cities using inexpensive wireless equipment and software freely available on the Internet, identified an unauthorized wireless device in one location, and had strong indications of three other wireless devices in other locations. The wireless access point located was not directly connected to the IRS network. However, anyone with a wireless detection tool could pick up the wireless signal and gain access to the computer. Also, if an employee connected to the access point with an IRS computer, and the access point was configured improperly, a hacker conceivably could gain access to the IRS network.

Furthermore, the IRS Computer Security Incident Response Center conducted penetration tests of the Enterprise Logistics Information Technology network. The penetration tests identified that one wireless access point was using a default configuration, security devices were not in place to detect attacks against the wireless network, and security configurations were not being monitored.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief, Mission Assurance and Security Services, use available tools to proactively scan, on a continuous basis, the entire IRS network for unapproved wireless devices and periodically advise employees of the risk involved with wireless technology. In addition, the Chief Information Officer should ensure the Enterprise Networks Division takes appropriate action to monitor and track the configuration files on the Enterprise Logistics Information Technology wireless network to ensure all files are set in accordance with the IRS wireless security policy.

In their response to the report, IRS officials agreed with the recommendations. The Mission Assurance and Security Services organization established a monthly wireless scanning project, initiated monthly scans in November 2006 that included nine IRS campuses and three IRS Computing Centers, and will expand the number of locations scanned after performing a risk-based evaluation. In addition, the Mission Assurance and Security Services organization will include information about the IRS wireless policy, risks associated with wireless technology, and the consequences for policy violations in the IRS' mandatory security awareness training. The Enterprise Networks Division is currently working with the Mission Assurance and Security Services organization to fully assess and manage the Enterprise Logistics Information Technology network devices to ensure all configurations adhere to IRS guidelines, standards, and procedures.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

http://www.treas.gov/tigta/auditreports/2007reports/200720060fr.pdf

Email Address: Bonnie.Heald@tigta.treas.gov
Phone Number: 202-927-7037
Web Site: http://www.tigta.gov